



INFORMATION DISCLOSURE
STATEMENT BY APPLICANT
Form PTO-1449 (Modified)
(Use several sheets if necessary)

Sheet

1

of

5

COMPLETE IF KNOWN	
Application Number	09/901,350
Confirmation Number	5351
Filing Date	JULY 9, 2001
First Named Inventor	Chawla
Group Art Unit	2135
Examiner Name	P. PICH
Attorney Docket No.	36321-8010.US01

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	U.S. Patent or Application		Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		NUMBER	Kind Code (if known)			
PP	4,386,416			Giltner	05/31/83	
	4,964,164			Fiat, Amos	10/1990	
	5,222,133			Chou et al.	10/17/91	
	5,557,712			Guay	02/16/94	
	5,734,744			Wittenstein	06/07/95	
	5,764,235			Hunt et al.	3/25/96	
	5,828,832			Holden et al.	10/27/98	
	5,848,159			Collins et al.	12/1998	
	5,923,756			Shambroom, W. David	7/1999	
	6,061,448			Smith et al.	5/2000	
	6,012,198			Anigbogu	02/01/00	
	6,073,242			Hardy et al.	06/06/00	
	6,081,598			Dai, Wei	06/2000	
	6,094,485			Weinstein, et al.	07/2000	
	6,098,096			Bayeh et al.	08/01/00	
	6,105,012			Chang et al.	8/2000	
	6,202,157			Brownlie et al.	03/13/01	
	6,154,542			Crandall	11/28/00	
	6,233,565			Lewis et al.	05/2001	
	6,233,577			Ramasubramani et al.	05/2001	
	6,237,033			Doeberl et al.	05/2001	
	6,396,926			Takagi, et al.	05/2002	
	6,397,330			Elgamal et al.	05/28/02	
	6,477,646			Krishna, et al.	11/2002	
↓	6,502,135			Munger et al.	12/2002	
	6,578,061			Aoki, et al.	06/2003	

EXAMINER <i>/Ponnoreay Pich/</i>	DATE CONSIDERED <i>06/16/2006</i>
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
Sheet	2	of	5	Application Number	09/901,350
				Confirmation Number	5351
				Filing Date	JULY 9, 2001
				First Named Inventor	Chawla
				Group Art Unit	2135
				Examiner Name	P. PICH
				Attorney Docket No.	36321-8010.US01

U.S. PATENT DOCUMENTS						
Examiner Initials*	Cite No.	U.S. Patent or Application		Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		NUMBER	Kind Code (if known)			
		6,584,567		Bellwood et al.	06/2003	
PP		6,587,866		Modi et al.	07/01/03	
		6,598,167		Devine et al.	7/2003	
		6,615,276		Mastrianni et al.	6/2004	
		6,621,505		Beauchamp	09/16/03	
		6,678,733		Brown et al.	1/2004	
		6,681,327		Jardin, Cary A.	1/2004	
		6,751,677		Ilnicki et al.	6/2004	
		6,757,823		Rao, et al.	06/2004	
		6,763,459		Corella, Francisco	07/2004	
		6,785,810		Lirov et al.	8/2004	
		6,874,089		Dick et al.	03/2005	
		6,886,095		Hind et al.	4/2005	
		6,941,459		Hind et al.	09/2005	
		6,963,980		Mattsson	11/16/00	
		6,990,660		Moshir et al.	1/24/06	
*		10/526,252		Fountain et al.	02-24/05	
*		10/850,827		Koyfman	05/20/04	
*		11/236,046		Metzger et al.	09/26/05	
*		11/236,294		Metzger et al.	09/26/05	
*		11/236,061		Metzger et al.	09/26/05	
		2002/0012473		Kondo et al.	9/30/1997	
		2002/0073232		Hong et al.	06/13/02	
		2002/0112167		Bokeh et al.	10/02/02	
		2002/0016911		Chawla et al.	07/09/01	
		2002/0039420		Schacham et al.	06/08/01	

EXAMINER	DATE CONSIDERED
/Ponnoreay Pich/	06/16/2006
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	09/901,350
				Confirmation Number	5351
				Filing Date	JULY 9, 2001
				First Named Inventor	Chawla
				Group Art Unit	2135
				Examiner Name	P. PICH
Sheet	3	of	5	Attorney Docket No.	36321-8010.US01

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.	U.S. Patent or Application		Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document
		NUMBER	Kind Code (if known)		
PP		2002/0066038		Mattsson	11/29/00
		2002/0087884		Shacham et al.	06/08/01
		2003/0014650		Freed et al.	01/16/03
		2003/0065919		Albert et al.	4/2003
		2003/0097428		Afkhami	05/22/03
		2003/0101355		Mattsson	12/28/01
		2003/0123671		He et al.	07/03/03
		2003/0156719		Cronce	02/21/02
		2003/0197733		Beauchamp	09/23/03
		2003/0204513		Bumbulis	10/30/03
		2004/0015725		Boneh et al.	07/24/02

FOREIGN PATENT DOCUMENTS					
Examiner Initials*	Cite No.	Foreign Patent or Application		Name of Patentee or Applicant of Cited Document	Date of Publication or Filing Date of Cited Document
		Office	NUMBER		
PP	*	WO	02/101605	Godfrey et al.	12/19/02

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS					
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published.			
PP	1.	Alteon Web Systems: "The Next Step in Server Loading Balancing" November 1999, Retrieved from the Internet: <u>URL: http://www.nortelnetworks.com/products/library/collateral/intel_int/webworking_wp.pdf</u> , Retrieved on March 2, 2004; pages 4-11.			
PP	2.	Alteon Web Systems: "Networking with the Web in Mind" May 1999, Retrieved from the Internet: <u>URL: http://www.nortelnetworks.com/products/library/collateral/intel_int/webworking_wp.pdf</u> , Retrieved on March 2, 2004; page 1, pages 3-7.			

EXAMINER <i>/Ponnoreay Pich/</i>	DATE CONSIDERED <i>06/16/2006</i>
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	09/901,350
				Confirmation Number	5351
				Filing Date	JULY 9, 2001
				First Named Inventor	Chawla
				Group Art Unit	2135
				Examiner Name	P. PICH
Sheet	4	of	5	Attorney Docket No. 36321-8010.US01	

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS						
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published.				T
PP	3.	Boneh, D., "Twenty Years of Attacks on the RSA Cryptosystem," Notices of the AMS, Vol 46, No. 2, pp. 203-213, 1999				
	4.	Boneh, et al., "An Attack on RSA Given a Small Fraction of the Private Key Bits," ASIACRYPT '98, LNCS 1514, pp. 25-34, 1998				
	5.	Boneh, et al., "Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$," (extended abstract), 1999				
	6.	Boneh, et al., "Efficient Generation of Shared RSA Keys," (extended abstract)				
	7.	Durfee, G., et al., "Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99," ASIACRYPT 2000, LNCS 1976, pp. 14-29, 2000				
	8.	Fiat, A. "Batch RSA, (digital signatures and public key krypto-systems)" Advances in Cryptology – Crypto '89 Proceedings 20-24 August, 1989, Springer-Verlag				
	9.	Großschädl, J., et al., "The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip," 2000				
	10.	Herda, S., "Non-repudiation: Constituting evidence and proof in digital cooperation," Computer Standards and Interfaces, Elsevier Sequoia, Lausanne, CH, 17:1 (69-79) 1995.				
	11.	Immerman, N., "Homework 4 with Extensive Hints," 2000				
	12.	Menezes, A., et al., "Handbook of Applied Cryptography," 1996 CRC Press, pp. §8.2-8.3 and §14.5				
	13.	RSA Laboratories: "PKCS #7: Cryptographic Message Syntax Standard, Version 1.5," RSA Laboratories Technical Note, pp. 1-30, November 1, 1993.				
	14.	RSA "PKCS #1 v2.0 Amendment 1: Multi-Prime RSA," 2000				
↓	15.	Schacham, H., et al., "Improving SSL Handshake Performance via Batching," Topics in Cryptology, pp. 28-43, 2001.				

EXAMINER /Ponnoreay Pich/	DATE CONSIDERED 06/16/2006
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	09/901,350
				Confirmation Number	5351
				Filing Date	JULY 9, 2001
				First Named Inventor	Chawla
				Group Art Unit	2135
				Examiner Name	P. PICH
Sheet	5	of	5	Attorney Docket No.	36321-8010.US01

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS						
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.				T
PP	16.	Shand, M., et al., "Fast Implementations of RSA Cryptography," 1993				
	17.	Sherif, M.H., et al., "SET and SSL: Electronic Payments on the Internet," IEEE, pp. 353-358 (1998)				
	18.	Stallings, W., "IP Security," Network Security Essentials, Applications and Standards, Chapters 6 and 7, pp. 162-223, 2000				
	19.	Takagi, T., "Fast RSA-Type Cryptosystem Modulo p^kq ," 1998				
	20.	Takagi, T., "Fast RSA-Type Cryptosystems Using N-Adic Expansion," Advances in Technology – CRYPTO '97, LNCS 1294, pp. 372-384, 1997				
↓	21.	Wiener, M., "Cryptanalysis of Short RSA Secret Exponents," 1989				

EXAMINER /Ponnoreay Pich/	DATE CONSIDERED 06/16/2006
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)		COMPLETE IF KNOWN	
		Application Number	09/901,350
		Filed	July 9, 2001
		First Named Inventor	Rajeev Chawla
		Group Art Unit	2131
		Examiner Name	Not yet assigned
		Atty Dkt No.	36321.8010.US01

FOREIGN PATENT DOCUMENTS

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published.	T
PP		"Security Protocols Overview (An RSA Data Security Brief)", RSA Data Security, 1999, http://www.directoryservice.com/WP/RSA/protocols.pdf , pages 1-4.	

EXAMINER /Ponnoreay Pich/	DATE CONSIDERED 06/16/2006
-------------------------------------	--------------------------------------

*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).